An Efficient JPEG Steganographic Scheme Using Uniform Embedding

Linjie Guo #1, Jiangqun Ni #2, Yun Qing Shi *3

School of Information Science and Technology, Sun Yat-Sun University
GuangZhou, GuangDong, P.R. China
1 g.linjie@gmail.com
2 issjqni@mail.sysu.edu.cn

* Department of Electrical and Computer Engineering, New Jersey Institute of Technology
Newark, New Jersey, USA
3 shi@njit.edu

***Abstract*—Steganography is the science and art of covert communication. Its objective is to hide the most secret messages into a cover object with the least possible statistical detectability. In practice, this is generally realized by a framework of minimal distortion embedding. This paper presents an efficient JPEG steganographic scheme based on syndrome trellis coding (STC) and a uniform embedding strategy, which, instead of random modification, tries to modify nonzero quantized DCT coefficients of different magnitude with equal probability, leading to possible minimal artifacts for statistics of DCT coefficients as a whole. The distortion metric corresponding to the uniform embedding is based on the magnitude of the DCT coefficients and both their intra- and inter-block neighborhood coefficients and known as uniform embedding distortion metric (UED). With the proposed scheme, the STC provides multiple codewords for a given message, while the UED determines the best one with minimal distortion. In this way, the average statistics change in each bin is significantly reduced, which corresponds to less detectability of steganalysis. Compared with prior arts, experimental results demonstrate the superior performance of the proposed scheme in terms of secure embedding capacity against steganalysis.**

I. Introduction

Steganography is the science and art of covert communication, in which the sender embeds secret message into the original image (cover) with shared key, and generates a stego image. To conceal the very existence of communication, the stego images have to be statistically undetectable from the cover images [1]. The undetectability and embedding payload, however, are two conflicting objectives that should be carefully considered when designing a steganographic scheme. Let n-dimensional vectors $\mathbf{x}$ and $\mathbf{y}$ denote the cover and stego objects, respectively, the cost of making an embedding change at element x_i be ρ_i, where $0 \leq \rho_i \leq \infty$, is the set of single letter distortions. With an additive distortion function, the overall impact after embedding is the sum of embedding cost at every element, i.e., $D(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} \rho_i(x_i, y_i)$. In practice, the problem is formulated as the one of minimal distortion embedding, i.e., to embed a given payload with minimal total embedding distortion D. For properly defined ρ_i, this will minimize the total statistical artifacts and thus make the resulting stego objects less detectable.

As a widely adopted format for image storage and transmission, JPEG steganography has become a domain of extensive research. There are a lot of schemes developed for JPEG steganography, such as F5 [2], nsF5 [3], MME [4] and some recently emerging adaptive algorithms [5][6]. In F5 [2], the embedding impact is treated as the same for each pixel, therefore minimizing the total distortion corresponds to the efforts to maximize the embedding efficiency, i.e., the number of message bits embedded per embedding change. F5 and its variants [3] improved the security performance by increasing its embedding efficiency through matrix encoding. Later, Kim et al. [4] proposed an improved scheme, called modified matrix encoding (MME), by only modifying the coefficients with less distortion. The nsF5 [3] tackles the issue of shrinkage with F5 by applying wet paper code (WPC). In [1] Filler et al. proposed a practical approach to minimizing embedding impact in steganography based on syndrome-trellis coding (STC), and have achieved an embedding efficiency close to the theoretical bound. By incorporating an additive distortion function defined by a set of local costs ρ_i, the STC framework can asymptotically achieve its performance bound. With the development of STC in steganographic code, it is increasingly recognized that further substantial increase in secure payload for steganography can only be achieved by properly designing the cost function instead of improving the coding scheme.

In [5], Sachnev et al. proposed an efficient JPEG steganographic scheme based on heuristic optimization and fast BCH syndrome coding which achieves significant improvement in security performance against steganalysis. Both the MME and the method in [5], however, require the original BMP image for steganography, which is not always available in practical applications. To represent the embedding cost at a coefficient x_i, Filler and Fridrich constructed a rich parametric model based on the coefficient itself and its neighborhoods [6]. By optimizing the model against the popular steganalysis feature set – CC-PEV-548D [7] and incorporating the STC framework [1], the proposed algorithm, which is known as MOD (Model Optimized Distortion), achieves significant improvement in terms of secure payload in DCT domain. Shortly after that, Kodovsky et al. demonstrated that the security of MOD can be compromised if the distortion is optimized to an incomplete feature space [8]. Recently, Kodovsky and Fridrich suggested using a rich model to detect JPEG steganography [9]. With the ensemble classifier [10], a huge feature set of up to 22,510-D can detect most existing JPEG steganographic schemes with high accuracy. As a result, the secure payload of JPEG steganography is decreased substantially, which poses new challenge on modern JPEG steganography.

A good JPEG steganographic scheme consists of an efficient steganographic coding and an effective distortion metric which well captures the statistical artifacts. In this paper, our major concern is then on the design of a new additive distortion metric for JPEG steganography. The proposed distortion metric follows the concept in spirit of "spread spectrum communication", and tries to guide the stego system to embed the messages to all nonzero quantized DCT coefficients of different magnitude with an equal probability, which leads to possible minimal statistical artifacts of DCT coefficients as a whole. It is noted that our proposed distortion metric is derived directly from the quantized block DCT coefficients; no original BMP image and pre-model training are required. By incorporating the new distortion metric with the STC framework, the proposed JPEG steganographic scheme performs quite well against the popular steganalyzers with feature sets, such as CC-PEV-548D [7], MP-486D [11], IBC-441D [8] and the new state-of-the-art feature set, CC-JRM-22510D [9].

The rest of this paper is organized as follows. In Section 2, the adaptive steganographic framework for minimal distortion embedding is briefly reviewed. The proposed distortion metric and the new JPEG steganographic scheme are presented in Section 3 and 4, respectively. The experimental results and analysis are provided in Section 5. Finally the concluding remarks are drawn in Section 6.

II. Practical Minimal Distortion Embedding Framework

In steganography, the transmitter communicates with the receiver by hiding her messages in seemingly innocent media, such as digital images, so that it is hard to distinguish the stego media from the cover ones. The message is generally hidden (embedded) in the cover image by slightly modifying some individual elements of cover (LSBs of pixels or quantized DCT coefficients, etc.). The problem of minimizing the embedding impact for single-letter distortion is well formulated in [1]. Let the binary vector $\mathbf{x}_b = (x_{b1}, x_{b2}, \cdots, x_{bn}), \mathbf{y}_b = (y_{b1}, y_{b2}, \cdots, y_{bn}) \in (0,1)^n$ and $\mathbf{m} = (m_1, m_2, \cdots, m_k) \in (0,1)^k$ represent the LSB vector of cover $\mathbf{x}$, LSB vector of stego $\mathbf{y}$ and message $\mathbf{m}$, respectively. The additive cost function is defined as

$$D(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} \rho_i(\mathbf{x}, y_i), \tag{1}$$

where $\rho_i(\mathbf{x}, y_i)$ is the cost of changing the ith cover element x_i to y_i. With the syndrome coding, the minimal distortion embedding framework is formulated as

$$\begin{aligned} Emb(\mathbf{x}, \mathbf{m}) &= \arg \min_{\mathbf{y}_b \in C(\mathbf{m})} D(\mathbf{x}, \mathbf{y}) \\ \text{and } H\mathbf{y}_b &= \mathbf{m} \end{aligned} \tag{2}$$

where H is parity-check matrix of the code C and $C(\mathbf{m})$ is the coset corresponding to syndrome $\mathbf{m}$.

III. Proposed Distortion Metric

A. Motivation behind uniform embedding strategy

JPEG steganalytic tools often take advantage of the distribution model of quantized DCT coefficients to construct feature set for steganalysis. And Laplacian distribution is a widely adopted model for quantized DCT coefficients. In practice, the histogram is considered as the first order statistics of the block DCT coefficients, while the co-occurrence matrix of the block DCT coefficients is often used as the second order statistics, which measures the correlations among the DCT coefficients.

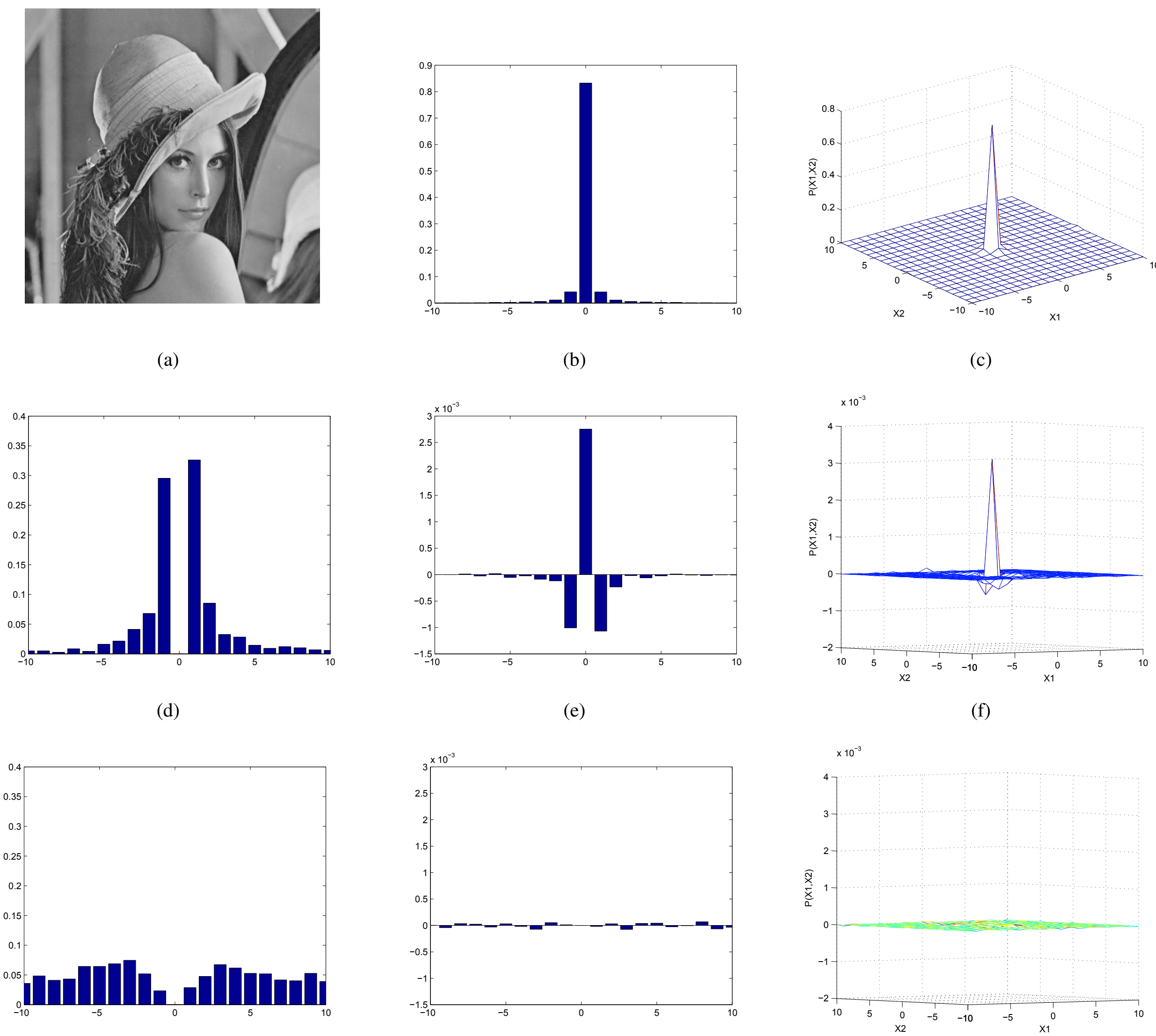
Once a secret message (payload) is embedded into a JPEG image, the statistics of the DCT coefficients will be modified to some extent, which leaves trace for steganalysis. The impacts of data embedding on the statistics of DCT coefficients are well illustrated with nsF5 [3] as shown in Fig.1, where Fig.1 (a) is the JPEG cover image 'Lena' with QF=75, Fig.1 (b) and Fig.1(c) are the global histogram h of DCT coefficients X and the co-occurrence matrix $P(X_1, X_2)$ of coefficient X_1 and its neighboring one X_2 with offset $d = (0, 1)$, respectively. For a given payload of 0.2 bpac, Fig.1 (d) is the histogram of the DCT coefficients which are selected to be modified by the nsF5 algorithm, while Fig.1 (e) and Fig.1(f) show the changes of h and $P(X_1, X_2)$ after nsF5 embedding, respectively. It is observed that most of the DCT coefficient modifications are taken place around bin zero, which can be easily explained by analyzing how nsF5 works.

The simulator of nsF5 embedding [3] first calculates the theoretical bound on the embedding efficiency according to the given payload α, and the number of modified coefficients n is obtained. The simulator then randomly selects n nonzero AC coefficients and decreases their absolute value by 1. Let $p(x)$ and $p_{\mathrm{nz}}(x)$ be the empirical probability density function (PDF) of the AC and nonzero AC coefficients, respectively. The number of AC coefficient at bin x, which needs to be modified, is $n \cdot p_{\mathrm{nz}}(x)$, thus the change of PDF after embedding is

$$\Delta p(x) = \begin{cases} n \cdot [p_{\mathrm{se1}}(x-1) + p_{\mathrm{se1}}(x+1)]/N & \text{if } x = 0 \\ n \cdot [p_{\mathrm{se1}}(x + \mathrm{sgn}(x)) - p_{\mathrm{se1}}(x)]/N & \text{if } x \neq 0, \end{cases} \tag{3}$$

where N is the total number of all the block DCT coefficients, and $p_{\mathrm{sel}}(x) = p_{\mathrm{nz}}(x)$ is the probability that coefficient x is selected.

Consider the fact that the block DCT coefficients are Laplacian distributed and the coefficients are selected randomly in nsF5, most of the non-zero AC coefficients and hence the modified ones are those with small magnitude, i.e., $|x| \leq 5$. Consequently, most of the coefficient modifications due to



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Fig. 1. Comparison in statistics changes between nsF5 and the proposed Scheme. (a) Cover image 'Lena'. (b) and (c) are the DCT coefficients histogram and the co-occurrence matrix distribution of neighboring DCT coefficients for cover image. (d) and (g) are the histograms for the modified coefficients with nsF5 and the proposed scheme at 0.2 bpac, respectively. (e) and (f) are changes in statistics of (b) and (c) with nsF5. (h) and (i) are changes in statistics of (b) and (c) with the proposed scheme.

this embedding strategy take place in the bins near zero. For 'Lena' image of QF=75, most of the non-zero quantized coefficients are located in bins with absolute magnitude 1 or 2 (i.e., $|x| = 1$ or 2), according to (3), the changes of statistics due to embedding in bin 0 and x ($|x| = 1$) are significantly larger than the ones in other bins as shown in Fig.1 (e)-(f).

Due to the distribution of DCT coefficients, most existing JPEG steganalysis tools, e.g. CC-PEV-548D [7], can achieve high detection accuracy by only monitoring the distribution artifacts of coefficients with small magnitude, even when the bin interval is only $[-2, 2]$. For JPEG steganography, although improving the coding efficiency would reduce the number of modified coefficients, it, however, would not radically change the distribution of modified coefficients. Therefore, the substantial statistics artifacts in DCT coefficients of small magnitude can still be easily detected by steganalysis tools when relatively large payload is required. To avoid the sudden change of statistics in coefficients with small magnitude, instead of random embedding, uniform embedding (UE) is more preferable as formulated in (4).

$$p_{\mathrm{sel}}(x + \mathrm{sgn}(x)) \cong p_{\mathrm{sel}}(x), x \in [-1024, ..., -1, 1, ..., 1024] \quad (4)$$

The uniform embedding strategy tries to "spread" the embedding modifications to coefficients of all possible magnitudes, so that the statistics change in each bin is minimized, i.e.,

$$\Delta p(x+\mathrm{sgn}(x)) \cong p(x), x \in [-1024, ..., -1, 1, ..., 1024]. \quad (5)$$

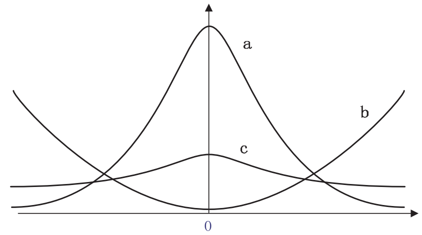


Fig. 2. Schematic illustration of the uniform embedding strategy. Curve 'a' is the distribution of DCT coefficients. Curve 'b' is the selection probability of each coefficient with UED. Curve 'c' is the distribution of the selected coefficients.

To embed a given message M, let ΔM be the total modifications, and RN and UN be the bin numbers involved in random and uniform embedding, respectively. The "spread magnitude" nature of uniform embedding makes $UN \gg RN$, therefore the average modification per bin ($\Delta M/UN$) for uniform embedding is much less than one ($\Delta M/RN$) for random embedding. It is noted that the proposed scheme neither modifies the zero-coefficients nor creates new zero-coefficients.

In practice, the uniform embedding strategy is implemented under the framework of syndrome trellis coding (STC) [1]. For a given message, the STC provides multiple codewords to embed it to a block of coefficients, a new distortion metric is incorporated to determine the one with least distortion. To actually implement the uniform embedding, the distortion metric known as uniform embedding distortion (UED) should be designed so that coefficients of different magnitude are equally selected. Let x denote the non-zero DCT coefficient, which is Laplacian distributed, i.e., the curve 'a' in Fig.2. The distortion metric used in UED should have the form of $\rho(x) = 1/|x|$, i.e., the selection probability of a coefficient x is increased with its absolute magnitude $|x|$ as shown by the curve 'b' in Fig.2. Curve 'c' in Fig.2 shows the near uniform distribution of selected DCT coefficients when the UED is incorporated, which also corresponds to the least detectability of steganalysis.

B. Distortion metric for the uniform embedding strategy

Let c_{ij} denote the DCT coefficient at (i, j), the distortion metric of form $1/|c_{ij}|$ is well explained with the concept of uniform embedding. To design the practical UED, however, the magnitudes of both the DCT coefficient itself and its intra- and inter-block neighborhood coefficients should be taken into account, as describe in (6).

$$\begin{aligned}\rho_{ij} = &\sum_{d_{\text{ia}} \in N_{\text{ia}}} \left(|c_{ij}| + |d_{\text{ia}}| + \alpha_{\text{ia}}\right)^{-1} \\ &+ \sum_{d_{\text{ir}} \in N_{\text{ir}}} \left(|c_{ij}| + |d_{\text{ir}}| + \alpha_{\text{ir}}\right)^{-1}\end{aligned}, \tag{6}$$

where α_{ia} and α_{ir} are adjustment parameters to satisfy the additive property and determined experimentally as 1.3 and 1, respectively; $N_{\text{ia}} = \{c_{i+1,j}, c_{i-1,j}, c_{i,j+1}, c_{i,j-1}\}$ and $N_{\text{ir}} = \{c_{i+8,j}, c_{i-8,j}, c_{i,j+8}, c_{i,j-8}\}$ are intra- and inter-block neighborhoods of coefficient c_{ij}, respectively. When the considered coefficient c_{ij} is located in the image boundary, the nonexistent coefficients are removed from (6) accordingly.

With the UED and STC framework, the statistics changes after steganography of 0.2 bpac for 'Lena' image are shown in Fig.1 (g)-(i). It is observed that the selected coefficients are much more uniformly distributed (Fig.1 (g)) than the ones with random selection in nsF5 (Fig.1(d)). Compared to Fig.1(e) and (f) of nsF5, the uniform embedding has a quite uniform distribution and much less average change of first and second order statistics, e.g., the global histogram and co-occurrence matrix with offset $d = (0, 1)$, as shown in Fig.1(h) and (i). No notable sudden changes in statistics is observed, especially in the region of small coefficients, say, $[-2, 2]$.

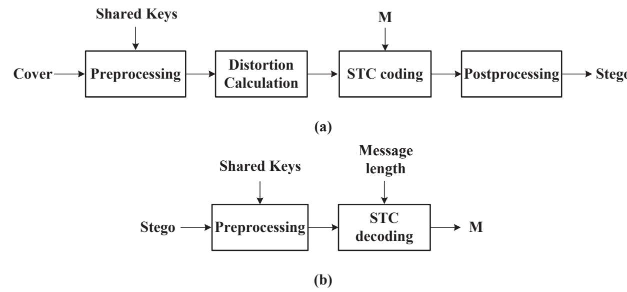


Fig. 3. Proposed scheme. (a) Data embedding. (b) Data extraction.

IV. Proposed JPEG Steganographic Scheme

The objective of minimal distortion embedding framework is to improve the security performance of steganography. To achieve this, syndrome coding based approach is usually employed. The proposed framework for JPEG steganography utilizes the syndrome-trellis coding (STC) [1] for data embedding, and the proposed distortion metric (UED) for embedding efficiency optimization, which includes the process of data embedding and extraction as shown in Fig.3.

A. Data embedding

1) Preprocessing: For JPEG image input, entropy decoding is applied to generate the quantized DCT coefficients. The non-zero AC coefficients are then scrambled with a shared key to obtain the cover coefficient $\mathbf{x} = \{x_i\}$.

2) Distortion calculation: Compute the embedding cost $\rho = \{\rho_i\}$ for each scrambled non-zero AC coefficient x_i using the proposed uniform embedding metric (6).

3) STC coding: Let the binary vector $\mathbf{m} = \{m_i\}$ and $\mathbf{x}_b = \{x_{bi}\}$ be the secret message and LSB of cover $\mathbf{x}$, respectively. With $\mathbf{m}$, $\mathbf{x}_b$ and its corresponding embedding cost ρ as input parameters, the STC coding is applied to embed secret message $\mathbf{m}$ to $\mathbf{x}$. The output of STC is the stego $\mathbf{x'}_b$ for $\mathbf{x}_b$, which is then used to construct the modified pattern $\mathbf{e} = \text{xor}(\mathbf{x}_b, \mathbf{x'}_b)$ of scrambled non-zero AC coefficients.

4) Postprocessing: Once the modified pattern $\mathbf{e} = \text{xor}(\mathbf{x}_b, \mathbf{x'}_b)$ is obtained, the cover is modified with (7) to obtain stego $\mathbf{y}$.

$$y_i = \begin{cases} x_i & \text{if } e_i = 0 \\ x_i + \mathrm{sgn(x_i)} & \text{if } e_i = 1 \& |x_i| = 1 \\ x_i \pm 1 & \text{if } e_i = 1 \& |x_i| > 1 \end{cases} \quad (7)$$

The entropy coding is then applied to generate stego JPEG image after $\mathbf{y}$ is descrambled.

B. Data extraction

1) Preprocessing: For a stego JPEG image, the quantized DCT coefficients are obtained by entropy decoding, which are then scrambled with the shared key to generate the scrambled non-zero AC coefficient $\mathbf{y}$.

2) STC decoding: The STC decoding is then applied to extract the hidden message $\mathbf{m}$.

V. Experimental results and analysis

Extensive experiments have been carried out to verify the feasibility and effectiveness of our proposed JPEG steganographic scheme, which include the comparisons with some recently proposed JPEG steganographic schemes, such as nsF5 simulator [3] and Filler and Fridrich's adaptive scheme with model optimized distortion (MOD) [6].

Our mother database is consist of 6680 uncompressed images including 3680 color images from the NJIT dataset and 3000 color images from NRCS [12]. All test images are first converted to grayscale ones, central-cropped into the size of 512×512, and finally JPEG compressed using quality factor 75. Thus, a databases of 6680 grayscale JPEG cover images with different textural characteristics, such as landscapes, people, plants, animals and buildings, is obtained. In the experiment, several mainstream universal JPEG-based feature sets, such as the CC-PEV-548D [7], MP-486D [11], IBC-441D [8] and the state-of-the-art CC-JRM-22510D [9], are employed to evaluate the security performances of the involved JPEG steganographic schemes. We test the security performance for different payloads ranging from 0.05 to 0.3 bpac with a step 0.05 at the typical quality factor $QF = 75$.

The ensemble classifier in [10] is employed in our experiments as is used in [9], since it enables fast training in high-dimensional feature spaces and has the comparable performance to SVMs [13] working on low-dimensional feature sets. For the cover and their corresponding stego images with different steganographic schemes and embedding rates, the feature sets for the above-mentioned three steganalysis tools are extracted, where half of the cover and the stego features are used as the training set for the ensemble classifier, and the remaining half are used as test set to evaluate the trained classifier. The minimal total error P_E under equal priors achieved on the test set is defined as

$$P_{\mathrm{E}} = \min_{P_{\mathrm{FA}}} \frac{P_{\mathrm{FA}} + P_{\mathrm{MD}}(P_{\mathrm{FA}})}{2}, \quad (8)$$

TABLE I
Detection errors of the involved schemes for different feature sets.

Features	Algorithm	0.05	0.10	0.15	0.20	0.25	0.30
CC-JRM	nsF5[3]	0.3561	0.1933	0.0808	0.0309	0.0103	0.0037
	MOD[6]	0.4088	0.2883	0.2299	0.1835	0.1431	0.1037
	UED	0.4595	0.3963	0.3307	0.2462	0.1698	0.0978
CC-PEV	nsF5[3]	0.3785	0.2418	0.1318	0.0611	0.0273	0.0117
	MOD[6]	0.4765	0.4275	0.3830	0.3360	0.2931	0.2370
	UED	0.4763	0.4328	0.3777	0.3050	0.2288	0.1486
MP	nsF5[3]	0.4234	0.3281	0.2355	0.1561	0.0984	0.0591
	MOD[6]	0.4813	0.4332	0.3815	0.3382	0.3147	0.2791
	UED	0.4891	0.4728	0.4427	0.4051	0.3526	0.2778
IBC	nsF5[3]	0.4642	0.4171	0.3684	0.3096	0.2551	0.2123
	MOD[6]	0.1638	0.0243	0.0073	0.0061	0.0061	0.0055
	UED	0.4783	0.4421	0.4099	0.3699	0.3159	0.2525

where P_{FA} is the false alarm rate and P_{MD} is the missed detection rate. The performance is evaluated using the median value of P_{E} over ten random tests and is denoted as $\overline{P_{\mathrm{E}}}$.

The security performances of different steganographic schemes against these four popular feature sets are summarized in Table 1, where the CC-JRM-22510D achieves the lowest detection error P_{E} when detecting the nsF5 and the UED. The performance comparisons among the involved schemes against the four feature sets are further illustrated in Fig.4. For CC-JRM-22510D and MP-486D, the proposed UED has a considerably better performance than that of nsF5, and outperforms consistently MOD under almost all tested payloads. It is noted that the MOD is optimized to CC-PEV-548D [7]. Under this circumstance, the UED still has a comparable performance with MOD when payload is less than 0.20 bpac and performs slightly better when payload is less than the secure payload (0.13 bpac, $P_{\mathrm{E}} \geq 0.4$) as shown in Fig.4(b). The more intriguing fact is that, for IBC feature set, which focus on detecting embedding changes of DCT coefficients with a large magnitude, the proposed UED also works best among involved schemes, and both the UED and nsF5 achieve significantly better performance than that of MOD as shown in Fig.4(d).

VI. Conclusion

Minimal-distortion embedding framework is a practical approach to implement JPEG steganography with high embedding efficiency. In this paper, an efficient JPEG steganographic scheme which utilizes syndrome trellis coding (STC) and uniform embedding (UE) strategy is presented. The uniform embedding is similar in spirit to spread spectrum communication. By "spreading" the embedding modifications to DCT coefficients of all possible magnitudes, the average statistics change in each bin is minimized, especially in the region of small coefficients, which leads to less detectability of steganalysis. A new distortion metric known as uniform embedding distortion metric (UED), which takes into account the magnitude of DCT coefficient as well as both its intra-

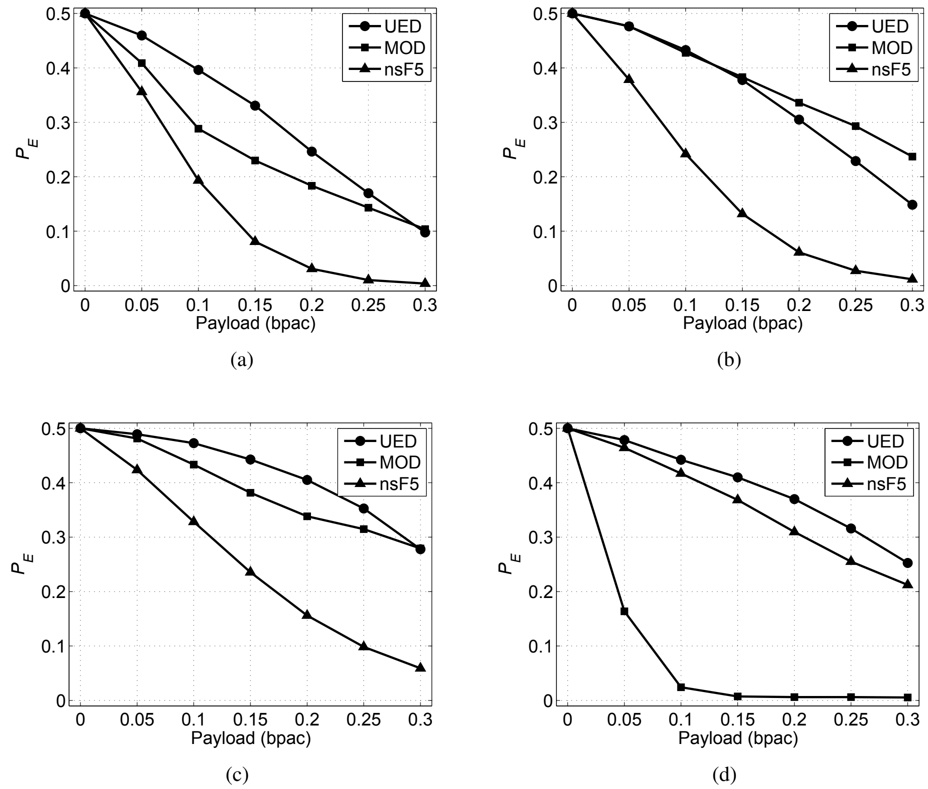


Fig. 4. Detection errors of the involved schemes as a function of payload for different feature sets. (a) CC-JRM-22510D. (b) CC-PEV-548D. (c) MP-486D. (d) IBC-441D.

and inter-block neighborhood coefficients, is constructed to incorporate the uniform embedding. Extensive experiments have been carried out to demonstrate the superior performance of the proposed scheme in terms of secure embedding payload against steganalysis.

ACKNOWLEDGMENT

The authors appreciate the support received from NSF of China under contract 60970145.

REFERENCES

[1] T. Filler, J. Judas, J. Fridrich, "Minimizing Additive Distortion in Steganography using Syndrome-Trellis Codes," *IEEE Transactions on Information Forensics and Security*, Volume 6, Issue 3, pp. 920–935, September 2011.

[2] A. Westfeld, "High capacity despite better steganalysis (F5-a steganographic algorithm)," *Information Hiding, 4th International Workshop*, LNCS 2137, pp. 289–302, 2001.

[3] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities," in *J. Dittmann and J. Fridrich, editors, Proceedings of the 9th ACM Multimedia & Security Workshop*, pages 3–14, Dallas, TX, September 20–21, 2007. Software available at http://dde.binghamton.edu/download/nsf5simulator/

[4] Y. Kim, Z. Duric, and D. Richards. "Modified matrix encoding technique for minimal distortion steganography," in *N. Johnson and J. Camenisch, editors, Information Hiding, 8th International Workshop*, volume 4437 of Lecture Notes in Computer Science. Springer-Verlag, New York, 2006.

[5] V. Sachnev, H. -J. Kim, R. Zhang, "Less Detectable JPEG Steganography Method Based on Heuristic Optimization and BCH Syndrome Coding," *Proceedings of the 11th ACM workshop on Multimedia and security*, pp. 131–139, Sep. 2009.

[6] T. Filler, J. Fridrich, "Design of adaptive steganographic schemes for digital images," *Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XIII*, San Francisco, CA, January 23–26, 2011.

[7] J. Kodovský and J. Fridrich, "Calibration revisited", in *Proc.11th ACM Multimedia Security Workshop, J. Dittmann, S. Craver, and J. Fridrich, Eds.*, Princeton, NJ, Sep. 7–8, 2009, pp. 63–74.

[8] J. Kodovský, J. Fridrich, and V. Holub, "On dangers of overtraining steganography to incomplete cover model," in *J. Dittmann, S. Craver, and C. Heitzenrater, editors, Proceedings of the 13th ACM Multimedia & Security Workshop*, pages 69–76, Niagara Falls, NY, September 29–30, 2011.

[9] J. Kodovský, J. Fridrich, "Steganalysis of JPEG Images Using Rich Models," *Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XIV*, San Francisco, CA, January 23–25, 2012.

[10] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble Classifiers for Steganalysis of Digital Media," *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 2, pp. 432–444, April 2012.

[11] C. Chen and Y. Q. Shi, "JPEG image steganalysis utilizing both intrablock and interblock correlations," *IEEE International Symposium on Circuits and Systems*, Seattle, WA, pp.18–21, May. 2008.

[12] NRCS Photo Gallery. Available: http://photogallery.nrcs.usda.gov/

[13] C. –C. Chang and C. –J. Lin, LIBSVM: a library for support vector machines, 2001. Available: http://www.csie.ntu.edu.tw/ cjlin/libsvm/